

UD

## UNITED STATES DISTRICT COURT

## SOUTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of

1102 La Mesa Blvd.  
Spring Valley, California

BY:

DEPUTY

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

CASE NUMBER:

05 mg 1331

I, Jason N. Smolanoff, being duly sworn depose and say:

I am a Special Agent of the Federal Bureau of Investigation and have reason to believe that on the property or premises known as:

See Attachment A-1

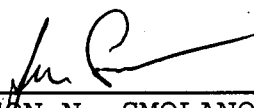
in the Southern District of California there is now concealed a certain person or property, namely:

See Attachment B

which is:

Evidence, contraband, fruits of crime, property designed for use or used in committing criminal offenses including violations of Title 18, United States Code, Sections 371, 2318 and 2320. The facts to support a finding of Probable Cause are as follows:

See attached Affidavit of Jason N. Smolanoff continued on the attached sheet and made a part hereof.  X  Yes       No

  
JASON N. SMOLANOFF  
Special Agent  
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence  
August 22, 2005 at San Diego, California:

  
HON. NITA L. STORMES  
UNITED STATES MAGISTRATE JUDGE

**AFFIDAVIT**

I, Jason N. Smolanoff, being duly sworn, hereby depose and state:

**INTRODUCTION**

1. I am employed as a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed for over five years. I am currently assigned to the Los Angeles Field Division Cybercrimes Squad, which is responsible for investigating computer and high-technology crimes, including those relating to intellectual property offenses.

2. During my career in the FBI, I have participated in investigations involving computer-related offenses, and have assisted with the execution of over thirty search warrants, the vast majority of which have involved searches and seizures of computers, computer equipment, software, and electronically stored information. I have received training in computer-related investigations and related issues from the FBI and private computer security companies, and have interviewed numerous individuals who have used computers in connection with criminal activity.

3. The FBI is currently conducting an investigation of ILONA and JAMES COCHRAN, doing business as Continuous Wave Technologies ("CWTECH"), PC PARTS, and www.go2pcparts.com, and others who are believed to be involved in manufacturing and/or trafficking in counterfeit computer programs and computer documentation.

4. This affidavit is submitted in the United States District Court for the Southern District of California in support of a warrant to search the following premises:

- a. CWTECH, 8801 La Mesa Boulevard, La Mesa, California 91941 ("SUBJECT BUSINESS") (as described in Attachment A-1 which is incorporated herein); and
- b. 1102 La Mesa Boulevard, Spring Valley, California 91977 ("SUBJECT RESIDENCE") (as described in Attachment A-2 which is incorporated herein) for evidence,

and/or instrumentalities of violations of 18 U.S.C. §§ 371, 2318 and 2320 as set forth

Attachment B ( which is incorporated herein ).

### **RELEVANT LEGAL STATUTES**

5. Title 18, United States Code, Section 2318(a) states, in pertinent part, that

Whoever, in any of the circumstances described in subsection (c) of this section, knowingly traffics in a counterfeit label affixed or designed to be affixed to . . . documentation or packaging for a computer program . . . and whoever in any of the circumstances described in subsection (c) of this section, knowingly traffics in counterfeit documentation or packaging for a computer program, shall be fined under this title or imprisoned for not more than five years or both.

Among the circumstances described in subsection (c) of Title 18, United States Code, Section 2318 are the circumstances that "the mail or a facility of interstate or foreign commerce is used or intended to be used in the commission of the offense" or "the counterfeit label is affixed to or encloses or is designed to be affixed to or enclose, a copy of a copyrighted computer program . . . ."

6. Title 18, United States Code, Section 2320(a) states, in pertinent part, that

Whoever intentionally traffic or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services shall, if an individual, be fined not more than \$2,000,000 or imprisoned not more than 10 years, or both . . . .

### **DESCRIPTION OF THE CD REPLICATION PROCESS, COMPUTER LICENSES, AND PRODUCT ACTIVATION**

7. The criminal activity relating to this investigation involves the production and distribution of computer software and counterfeit computer documentation. In order to better understand the nature of the criminal activity involved, I describe below my understanding (as obtained through information provided by various representatives of Microsoft, Symantec, Adobe, and individuals knowledgeable with respect to high-volume software production) of both

the CD replication process, which can be used to manufacture counterfeit software, as well as the nature of documentation in the form of licenses that confer the right to use authorized software:

a. CD Replication Process: A compact diskette ("CD") is composed of molded polycarbonate and a thin film of aluminum. CD replication is a manufacturing process that replicates an original set of data using a technique called "stamping." All digital media (including CDs) store data in binary code that is susceptible to interpretation by a computer. In a binary code number system, there are only two possible states, off and on, usually symbolized by 0 and 1. In physical terms, binary code -- the series of 0's and 1's -- is expressed on the surface of a CD as "valleys" or "hills," i.e., depressions or elevations. Thus, it is possible to replicate the data from an original CD master by replicating the "valleys" and "hills" -- the physical expression of the binary code -- onto a duplicate CD. This replication process involves recreating the desired data -- the desired sequence of "valleys" and "hills" -- on a glass substrate that is then used to create multiple metal stampers. A metal stamper comprises the negative impression of the glass master disk and therefore a negative impression of the original data set that is to be replicated. The metal stamper is mounted into a CD replication machine, where it presses or "stamps" the original data set into molded polycarbonate. The stamped and molded polycarbonate, which is in the form of a disk, is cooled and coated with a reflective aluminum coating. The entire CD is then encapsulated with a protective epoxy coating. When the disk is placed into a CD player, a laser inside the player "reads" the series of "valleys" and "hills" on the CD surface, interpreting them as a series of 0's and 1's constituting a set of data. High-volume CD replication requires a technologically complex CD replication system along with a silk-screening machine to apply artwork directly to the CD. Typically, such systems are capable of producing approximately 8,000 CDs in a twelve-hour period.

b. Computer Licenses: For purposes of this investigation, three types of computer documentation are relevant -- the Client Access License ("CAL"), the End User License Agreement ("EULA"), and the Certificate of Authenticity ("COA") (for purposes of simplicity, this affidavit will use the term "license" when referencing either CALs, EULAs, or COAs):

i. A EULA is a document or agreement in which a software company/developer grants permission to use its software according to certain conditions. Typically, the EULA is presented electronically during the software installation procedure or on a piece of paper that accompanies a new, shrink-wrapped software package. The user has the choice of accepting or rejecting the agreement. Installation and use of the software is conditioned on the user accepting the agreement and agreeing to abide by its terms.

ii. A CAL authorizes multiple users or devices to access a single copy of software that is installed on a computer mainframe or server configuration. A CAL is required for each user or device (or combination of both) that accesses or uses the software and is accompanying documentation authorizing the use of particular software. As an example, Microsoft is a corporation engaged in the business of developing, promoting, advertising, marketing, distributing and licensing computer software programs. Among Microsoft's many computer programs are Microsoft Windows Server 2003, Microsoft SQL Server 2000 and Microsoft Office 2000. Microsoft distributes this software for sale to the public in a package with several components, including, among other things, diskettes and/or CD-ROM, an accompanying EULA, a COA, and packaging materials. Customers interested in using multiple copies of a certain type of software need not purchase a large number of the packaged software and materials. Instead, such customers have the alternative of purchasing software with

additional licenses -- one type of which is the CAL -- to enable access by additional users. Thus, a business may purchase a single software package, which only authorizes a single user, and may purchase additional license rights which authorize the business to install and operate the software on a specified number of additional computers for a specified number of additional users.

iii. A COA is a document included with a software program that certifies the program was purchased legally and often has a unique identification number (typically a product activation key code) used by the software for activation subsequent to a new installation.

c. Software Product Activation: Software product activation is intended to deter individuals from violating software copyright laws and unauthorized copying of protected intellectual property (for example, installing multiple copies of a computer program in violation of the licencing agreement). Product activation has many different levels of complexity, but in the case of the Microsoft Windows XP operating system, product activation is achieved using a software algorithm (included in the software) and a product key code (typically found printed on a COA). The algorithm is simply a mathematical function that uses the product key code to create a unique number, that is transmitted via the Internet, to a Microsoft authentication server. If the key code is authentic, the Microsoft authentication server will transmit a signal activating the software. If the key code is not valid, the software will not fully install on the computer and will wait for a valid key code entry. A typical Microsoft Windows XP product key code is comprised of a combination of twenty five integers and alphanumeric symbols. All new purchases of Microsoft Windows XP software include a compact disk (containing the software), an end-user license agreement, a warranty card, and a product activation code (key code). In the case of Microsoft Windows XP software, an authentic product key code will be printed on a

certificate of authenticity (COA) that is typically displayed on a computer case.

### **OPERATION DIGITAL MARAUDER**

8. Between June 2003 and August 2004, I was the case agent for Operation Digital Marauder ("Marauder"), an FBI undercover operation which targeted members of an extensive criminal enterprise involved in the manufacture and distribution of counterfeit computer software products, in violation of Title 18 USC 2318 (Trafficking in Counterfeit Computer Documentation); Title 18 USC 2320 (Trafficking in Counterfeit Goods); and Title 17 USC 506, (Criminal Copyright Infringement). The illegal enterprise spanned over a large geographical area including Los Angeles, San Francisco, Seattle, Austin, and Hong Kong. On August 26, 2004, I participated in a coordinated law enforcement action that culminated in the arrest of fourteen individuals, and the execution of search warrants in Austin, Texas, and San Francisco, California. The investigation yielded approximately \$87 million in counterfeit software (which included titles from among others, Microsoft, Symantec, and Adobe), compact disk (CD) replication equipment, printing equipment used to manufacture counterfeit software products, and numerous documents that identified at least thirty or more companies and associated Internet websites located throughout Southern California and the United States which consistently purchased and distributed counterfeit software. Based on previous contact with the Microsoft, Symantec, and Adobe corporations, and information obtained during the course of Operation Digital Marauder (including information obtained through numerous undercover transactions relating to the sale and purchase of counterfeit Microsoft, Symantec, and Adobe software), the FBI has identified companies that are knowingly procuring counterfeit software products.

9. During the course of our dealings with the target companies directly involved in Operation Digital Marauder, I found that they dealt solely in the procurement and distribution of

counterfeit software. A confidential source (CS-1), who was a primary target in the Marauder investigation, confirmed this conclusion, admitting that his/her companies were dealing, almost exclusively, in procuring and distributing counterfeit and non-genuine software.

10. Additionally, CS-1 has confirmed that the thirty or more companies and associated Internet websites (identified in Operation Digital Marauder) as procurers of counterfeit software products had, in fact, been customers of his/her company.

**CONFIDENTIAL SOURCE (CS-1)**

11. As set forth above, CS-1 was a primary target in Operation Digital Marauder. CS-1 is well known and has vast contacts in the counterfeit software community. CS-1 has spent over a decade acquiring and distributing counterfeit and non-genuine software products. CS-1's ability to identify companies and individuals who are involved in the distribution and procurement of counterfeit software products, in my opinion based upon my training and experience, is very unique. CS-1 has pled guilty to conspiracy, in violation of 18 U.S.C. § 371, and trafficking in counterfeit computer documentation, in violation of 18 U.S.C. § 2318, and has agreed to cooperate in the Government's ongoing investigations. I, and other Government representatives, have debriefed CS-1 extensively, and have corroborated much of the information. Currently, CS-1 is operating under my direction to identify, and gather evidence, against various individuals and companies identified during Operation Digital Marauder.

12. On or about March 2005, I became the case agent for a second undercover investigation, whose goal is to investigate the companies identified during Operation Digital Marauder. Among others, I am currently investigating ILONA and JAMES COCHRAN, d.b.a. CWTECH. In furtherance of this investigation, beginning on or about June 2005, I directed CS-1 to re-establish contact with ILONA COCHRAN. During



numerous consensually recorded telephone conversations and electronic mail (e-mail) correspondence throughout this investigation, ILONA COCHRAN repeatedly and consistently discusses, with both CS-1 and an undercover FBI agent (UCE), the distribution and procurement of counterfeit and non-genuine Microsoft software products, including compact disks containing copyrighted software, user manuals, EULA's, CAL's, and COA's. ILONA COCHRAN discusses pricing, shipping, and payment terms for counterfeited or non-genuine software products. Unless indicated otherwise, all of the telephone calls described in this affidavit involving CS-1 were consensually recorded. The conversations which take place with the UCE occur via e-mail, in which COCHRAN believes she is speaking with CS-1 about their ongoing business dealings.

13. The facts set forth below are based upon my own personal observations and knowledge, my training and experience, and reports and information provided to me by others, including law enforcement officers and individuals employed by or on behalf of Microsoft. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of an application for a search warrant, it does not set forth each and every fact known by me and others relating to this investigation. Furthermore, unless specifically indicated otherwise, all conversations and statements described in this affidavit are not related verbatim, but are related in substance and in part only.

#### **BACKGROUND PROBABLE CAUSE**

14. In or around the Spring of 2004, SA Robin Davis reviewed shipping records provided by FedEx and told me the following:

a. She reviewed the FedEx shipping records for Data Consulting Services, aka Smart Software Sales, aka FBSS Technologies (collectively, the

"Marauder Companies"), which were fictitious business names for a single company owned and operated by several Marauder defendants. The Marauder Companies conducted thousands of shipping transactions between 2003 and 2004 with various companies throughout the United States. It should be noted that during the investigation, these companies dealt exclusively in the sale and purchase of counterfeit software products.

b. Analysis of these shipping records identified the top ten companies in the California area with the largest volume of transactions. Specifically, the analysis identified hundreds of product shipments (both sent and received) between various MARAUDER defendants and both JAMES AND ILONA COCHRAN, at CW TECH, 8801 La Mesa Boulevard, La Mesa, California 91941 (THE SUBJECT BUSINESS) and ILONA COCHRAN, aka CW TECH, at 1102 La Mesa Avenue, Spring Valley, CA 91977 (THE SUBJECT RESIDENCE).

i. According to public database records, THE SUBJECT RESIDENCE is owned by JAMES COCHRAN AND ILONA COCHRAN.

ii. According to public database records, Continuous Wave Technologies is an active, registered company with the State of California. JAMES COCHRAN is listed as the president with a corporate mailing address of 8801 La Mesa Boulevard, La Mesa, California (THE SUBJECT BUSINESS).

15. In and around Summer of 2004, SA Robin Davis reviewed a second set of records provided by FedEx corporation and told me the following:

a. Thomas Polmatier, a Marauder defendant and the owner of Ideal Data, 3021 NE 72nd Drive, Suite 9, Vancouver, Washington, has a FedEx account.

Polmatier was conducting a high volume of shipping transactions, both sending and receiving, with ILONA COCHRAN, aka CW TECH.

16. A review of sales receipts and documents seized from defendants in Austin, Texas during the execution of Federal search warrants on August 26, 2004 revealed that CWTECH paid approximately \$119,000 to the MARAUDER defendants for counterfeit and/or non-genuine software between April 2004 and August 2004. This was also confirmed during my conversations with CS-1. Had the software products been genuine, the software products purchased by CWTECH would have an approximate retail value of over \$1 million.

a. Additionally, documents seized during the August 26, 2004 searches revealed that CWTECH's business relationship with the Marauder defendants dated back to at least 2003. One of many documents that I reviewed illustrates CWTECH's knowledge regarding the type of software they were purchasing from the Marauder defendants.

i. For example, I reviewed a document with the heading CWTECH, Inc. 8801 La Mesa Blvd., La Mesa, CA 91941 (the SUBJECT BUSINESS), telephone number (619) 337-8805, dated August 18, 2003. The document was notification to the MARAUDER defendant's company that CW TECH was returning items previously purchased. One item returned was a Microsoft product, *Front Page 2000*, a computer software program used for website design. The reason for the return was "bad key code". The letter was signed by JIM COCHRAN.

ii. In my training and experience, a legitimate software reseller understands that a "bad key code" is an indication of a counterfeit COA. Legitimate

resellers would not continue a business relationship with a company who is selling counterfeit software and are advised (by software manufacturers) to report the incident to Microsoft, Symantec, Adobe, and law enforcement. This information indicates that despite receiving counterfeit software products, CW TECH continued to conduct business with the MARAUDER defendants

17. On or about March 2005, I was contacted by Microsoft Investigator Thomas Montgomery who told me that Microsoft Corporation has been conducting an anti-piracy investigation regarding CW TECH since 2001. Information obtained during Microsoft's investigation, as related to me by Montgomery, regarding CW TECH is summarized below:

a. CW TECH is owned and operated by JAMES AND ILONA COCHRAN. They use both the SUBJECT BUSINESS address and the SUBJECT RESIDENCE address, and telephone numbers (619) 337-8805 and (619) 460-7284, respectively, to buy and sell software products. According to Microsoft, the telephone numbers are land lines that trace to the respective business and residence and are both subscribed to JAMES COCHRAN.

b. CW TECH uses an Internet website named [www.go2pcparts.com](http://www.go2pcparts.com) to sell both genuine, non-genuine, and counterfeit software. A public Internet domain registry search revealed that this website is registered to CW Technologies, aka James Cochran, at THE SUBJECT RESIDENCE.

i. In my training and experience and through conversations with software industry representatives, non-genuine software refers to genuine software that has been re-labeled. For example, software companies sell academic versions of

software at a significantly lower price than the retail version, although there is not difference in the software content between the academic and retail versions. Individuals and companies, involved in the resale of non-genuine products, will purchase the academic version, remove the academic version labels from the software and licences, and then resell the re-labeled or non-genuine software for the retail price.

c. Between July 2001 and August 2005, Microsoft received 71 total reports regarding suspected counterfeit software sales from CW TECH. 65 of the reports were from suspect Internet sales. A portion of the suspected Internet sales are from the website [www.go2pcparts.com](http://www.go2pcparts.com). The reports are made by customers and Microsoft investigators.

d. Microsoft, and/or their authorized agents, routinely analyze software to determine if it is genuine and authentic. The suspect software is typically submitted by Microsoft investigators, law enforcement, and/or customers. To date, Microsoft has analyzed approximately fifteen different software submissions (from Microsoft Test Purchases, Customer Submissions, and Law Enforcement) for software purchased from CW TECH. Microsoft and/or their authorized agents, have determined that fourteen of the fifteen software submissions are either counterfeit, or non-genuine products (for example, products that have all of the genuine security features, but the labels have been changed to reflect a different product).

e. On or about September 20, 2001, Microsoft sent a "warning letter" to Go2PCParts, aka CW TECH, at THE SUBJECT RESIDENCE. A warning letter informs a company or individual that Microsoft has received a report that the company may have distributed illegal and/or unlicensed Microsoft software. The letter explains

how the company can avoid distributing counterfeit and other forms of illegal software. The letter describes in detail how a company can avoid becoming involved in different types of software piracy. Additionally, the letter describes the correct procedures for distributing Microsoft software and licensing.

f. On or about September 28, 2001, Microsoft sent a "Cease and Desist" (C&D) letter regarding the illegal distribution of counterfeit Microsoft software to Go 2 PC Parts.com, aka CW TECH, to THE SUBJECT RESIDENCE. The letter was sent by certified mail and signed for by ILONA COCHRAN. The C&D letter stated that CW TECH was in violation of Federal and State trademark and copyright laws for distributing counterfeit Microsoft software.

#### **SUMMARY OF THE CURRENT INVESTIGATION**

18. In light of the information obtained from Microsoft and the Marauder investigation, I directed CS-1 to contact ILONA COCHRAN. CS-1 confirmed that ILONA COCHRAN, aka CWTECH, was a prior customer who had purchased a high volume of counterfeit and non-genuine software products during the Marauder investigative time frame.

19. On or about June 23, 2005, CS-1, acting at my direction, attempted to contact ILONA COCHRAN at telephone numbers (619) 337-8805 and (619) 460-7284. These telephone numbers are land lines linked to THE SUBJECT BUSINESS and THE SUBJECT RESIDENCE, respectively.

a. Public records, Internet, and public database inquiries revealed the following information:

i. The telephone number (619) 460-7284 is listed to JAMES

COCHRAN, 1102 La Mesa Avenue, Spring Valley, CA 91977 (THE SUBJECT RESIDENCE).

ii. Continuous Wave Technologies, aka CWTECH, is listed in the LaMesaCityGuide.com website. The contact information is: JAMES COCHRAN, 8801 La Mesa Boulevard, La Mesa, CA 91941, telephone number (619) 337-8805 (THE SUBJECT BUSINESS)

20. On or about June 23, 2005, CS-1 spoke with ILONA COCHRAN using the SUBJECT RESIDENCE telephone number, (619) 460-7284. During this phone call, among other things, CS-1 discussed pricing, methods for obtaining "brown box" software products, and the current state of the software market. Cochran stated that she is looking for compact disks (for example Microsoft Windows 2003 Server and Microsoft Visual Studio products) and other "brown box" products (described below). During this conversation, Ilona Cochran provided CS-1 with her e-mail address, icochran@cox.net and cell phone number, (619) 208-7167.

a. In my training and experience, and through discussions with CS-1, I understand that the term "brown box" is common term in the counterfeit software community. "Brown box" software products are typically a complete software package that contains CD's, licenses, COA's, and associated manuals that are sold in a non-retail box. The software components are typically all counterfeit or a mixture of counterfeit and genuine products. This product is typically sold at a highly discounted rate from the true retail price (for example, Microsoft SQL Server 2000 Enterprise Edition has a retail price of \$19,999 as found on the Microsoft website; The counterfeit "brown box" version was sold to CWTECH for \$2,500. This transaction is described in more detail below).

21. On or about June 27, 2005, an FBI undercover employee (UCE), posing as CS-1, provided ILONA COCHRAN the e-mail address softwareptbb@earthlink.net and requested that all future e-mail correspondence use this e-mail account. This e-mail account is under the control of the FBI, and only FBI personnel have access to it. ILONA COCHRAN's e-mail address is icochran@cox.net. This account is hosted by Cox Communications.

22. On or about August 10, 2005, I spoke with and received a facsimile from Kenya Nelson, a paralegal for Cox Communications. Kenya Nelson told me that the e-mail address icochran@cox.net is associated with an active high speed Internet service account provided by Cox Communications. When this account was initially activated, Cox provided the account subscriber, JAMES COCHRAN using THE SUBJECT RESIDENCE address (telephone number 619-460-7284), with a cable modem to access the Internet. According to Nelson, there is only one cable modem that is accessing the Internet using JAMES COCHRAN's account.

**MICROSOFT WINDOWS OFFICE 2003 NOT FOR RESALE (NFR)**  
**TRANSACTION**

23. Between June 28, 2005 and July 1, 2005, ILONA COCHRAN had several contacts with CS-1 and the UCE via telephone and e-mail, respectively. A summary of the conversations and correspondence is below:

a. Cochran wanted to purchase fifty pieces of Microsoft Windows Office 2003 Professional (Office 2003 Pro). Cochran wanted to know if key codes are included with the CD's; what does the CD package include; and what is the cost per piece. The UCE stated that the Microsoft Office 2003 CD's do not have product key



codes, but the UCE can obtain them quickly. Cochran then inquired about what type of product is the Microsoft Office 2003 Pro CD's, are they retail product or Original Equipment Manufacturer ("OEM") (OEM is briefly described below). The UCE replied that the Microsoft Office 2003 product was Not for Resale ("NFR") and would cost \$140 per piece. Cochran ordered three pieces of Office 2003 Pro Not for Resale (NFR) CD packs with product key codes for \$140 per pack, and stated that she would probably order another fifty.

i. In my training and experience, a legitimate distributor or reseller of computer software would not have this type of conversation. All genuine and authentic computer software includes a CD, a COA that includes a product key code, a EULA and/or CAL, and is typically packaged in shrink wrap. OEM software is specifically licensed to computer hardware manufacturers (for example, Dell Corporation) for distribution with the sale of new computer hardware. This software is not licenced for sale without a new computer. In addition, a legitimate computer software reseller of Microsoft products is aware of licencing restrictions for selling OEM software products. Resellers and distributors of Microsoft products, in most cases, are made aware by Microsoft, that they cannot purchase Microsoft Office 2003 Pro NOT FOR RESALE (NFR) CD's. NFR CD's are not for resale, and are obtained only when purchasing a volume license agreement from Microsoft. Additionally, legitimate resellers and distributors of retail computer software would know that the price that CS-1 requested for the Microsoft Office 2003 Professional software (\$140 per box) is far below the full retail price set by Microsoft. According to Microsoft, the full retail price for Office 2003 Pro retail software is \$499.

ii. Further, ILONA COCHRAN was notified of Microsoft's licencing practices in the warning and C&D letters she received in 2001 which should have made apparent that authorized software is not distributed without valid key codes.

b. On July 1, 2005, I sent three Office 2003 Pro CD packs with product key codes via FedEx to CW TECH, attn: ILONA, at the SUBJECT BUSINESS address. I placed three invalid key codes, printed on individual stickers, on each CD package.

c. On or about July 8, 2005, I received a package from CW TECH, using THE SUBJECT BUSINESS as the return address. Among other items, the package contained a check in the amount of \$430, drawn upon the account of CW TECH at Wells Fargo Bank. In the memo section of the check, the notation "3 OFFC 2003 PRO" was written. The signature on the check appeared to read J. COCHRAN.

d. On or about July 14, 2005, the UCE received an e-mail from ILONA COCHRAN, aka icochran@cox.net. The following is a summary of the e-mail: Ilona has three bad Microsoft Office 2003 Professional CD's, and the key codes are invalid. Can CS-1 replace them or send three valid key codes. On the same day, a second e-mail was received by the UCE from ILONA COCHRAN. The e-mail contained the invalid key codes. These codes were the same numbers as the ones that I placed on the disks that were originally sent to ILONA COCHRAN.

e. Between July 14, 2005 and August 8, 2005, the UCE received approximately three more e-mails requesting the correct product key codes. If the UCE could not obtain valid product key codes, ILONA COCHRAN would cancel the order, return the three disk sets, and request a refund.

f. On or about August 11, 2005, I received the three Microsoft Office 2003 Professional NFR CD's. ILONA COCHRAN returned the disks using FedEx and THE SUBJECT BUSINESS as the return address. The package was sent Cash On Delivery for \$430. The UCE provided a check made payable to CW Technologies as a refund for the returned product.

#### **MICROSOFT SQL SERVER 2000 ENTERPRISE TRANSACTION**

24. Between June 28, 2005 and July 1, 2005, I reviewed several consensually recorded telephone calls and e-mails between ILONA COCHRAN and CS-1 and the UCE, respectively. A summary of the contacts are below:

a. ILONA COCHRAN requested a quote for eight pieces of Microsoft SQL Server 2000 Enterprise Processor:1 (SQL ENTERPRISE) bundles (a bundle refers to a package containing CD's, EULA, COA, and manual). ILONA COCHRAN requested that the source give her a "real good price". The UCE responded, via e-mail, and inquired if ILONA "wanted the really expensive ones or the cheaper ones". COCHRAN indicated that she wanted the product to look good.

i. In my training and experience a legitimate distributor or reseller of computer software would not discuss the quality of the product. All legitimate resellers purchase product from Microsoft or an authorized Microsoft distributor. Microsoft has a quality control plan in place to assure all purchasers of their products receive the same level of quality. Only resellers knowingly purchasing counterfeit or non-genuine software products would discuss their quality.

b. CS-1 told ILONA COCHRAN that each bundle would cost \$2,500 and she ordered eight bundles. The bundles were shipped to ILONA COCHRAN via

FedEx at THE SUBJECT BUSINESS . The bundles contained a set of CD's, a EULA, a COA, and a manual. The software components were placed in one box, without any retail packaging.

c. On July 8, 2005, I received a package from CWTECH using THE SUBJECT BUSINESS as a return address. Among other items, the package contained a check in the amount of \$20,200 drawn upon the account of CWTECH at Wells Fargo Bank. In the memo section of the check, the notation "8 SQL 2K ENT " was written. The signature on the check appeared to read J. COCHRAN.

d. SQL ENTERPRISE is typically sold in a shrink wrapped retail box. A legitimate copy and license for SQL ENTERPRISE has a retail value of \$19,999, as listed on the Microsoft website. In my training and experience a legitimate distributor or reseller of computer software would suspect that the SQL ENTERPRISE they purchased for \$2,500 is not genuine based upon the low price and packaging.

#### **VISUAL BASIC/VISUAL STUDIO/ OFFICE 97 PURCHASE**

25. On or about June 30, 2005, I reviewed an e-mail between ILONA COCHRAN, using the e-mail address icochran@cox.net, and the UCE, where she provided prices for three products, Microsoft Visual Basic 6.0 Professional (Visual Basic), Microsoft Visual Studio 6.0 Professional (Visual Studio), and Microsoft Office 97 (Office.97). The cost for each product was \$350, \$465, and \$175, respectively.

a. CS-1 ordered one piece of Visual Basic, one piece of Visual Studio, and five pieces of Office 97 from CW TECH and agreed to pay \$1,715 for these products.

b. On or about July 8, 2005, I received two packages via Federal

Express. The package was shipped from CW TECH, using THE SUBJECT BUSINESS and telephone number (619) 337-8805 as a return contact. The packages contained, among other things, the following computer software:

i. Microsoft Visual Studio 6.0 Professional CD case containing 3 compact disks, Microsoft Visual Basic 6.0 Professional CD case containing 1 compact disk, 2 sets of Microsoft Visual Studio 6.0 Library CD case containing 2 compact disks, 2 sets of Microsoft Visual Studio Developing for Windows and the Web Guide, assorted Microsoft software licenses and notices, and five pieces of Office 97.

c. The retained evidentiary samples of the Visual Basic, Visual Studio, and Office 97 discussed in the paragraphs above were later submitted to Microsoft and/or its representatives for analysis. Based on information received in connection with that analysis, I learned the following:

i. All of the sample Visual Studio and Visual Basic CD's and licenses were counterfeit.

(1) All of the sample licenses bore identifying labels that appeared to be genuine Microsoft labels, but were not, as well as counterfeit marks, namely, spurious marks identical to and substantially indistinguishable from Microsoft trademarks, which are in use and are registered for use on licenses on the principal register of the United States Patent and Trademark Office, the use of which is likely to cause confusion, to cause mistake and to deceive.

(2) Based on my review of the retained counterfeit licenses from this transaction and information provided to me by Microsoft, it appears that all of the sample counterfeit software products bore identifying labels that appeared to be genuine Microsoft labels, but were not, as well as counterfeit marks, namely, spurious marks identical to and substantially indistinguishable from Microsoft trademarks, which are in use and are registered for use on licenses on the principal register of the United States Patent and Trademark Office, the use of which is likely to cause confusion, to cause mistake and to deceive.

ii. All of the Office 97 CD's and licences were genuine. In my training and experience, I know that this is a common tactic for resellers of counterfeit software products. Most companies sell a mixture of counterfeit and genuine software products to conceal, from software manufacturers and law enforcement, their full knowledge regarding the type of products they are distributing.

#### **COMPUTER DATA**

26. Based upon my training, experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know

that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in

desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million pages of data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

#### **Items To Be Seized**

27. Items constituting evidence of violations of Title 18, United States Code, Sections 371, 2318 and 2320, including the following:

a. All computer software, computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) and software licenses (such as client access licenses or end user licenses) bearing any identifying label or mark used by Microsoft, Symantec or Adobe that appears genuine,



but is not.

b. All computer software, computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) and software licenses (such as client access licenses or end user licenses) determined to be, or suspected by appearance and/or price to be, counterfeit, fraudulently obtained, or altered.

c. All tools, devices, implements, materials, mechanical equipment and tangible things capable of being used in connection with processes to replicate, manufacture, label or otherwise produce documents that appear virtually indistinguishable from genuine computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) and software licenses (such as client access licenses or end user licenses) offered by Microsoft, Symantec or Adobe.

d. All documents and records from August 1, 2003 through the date of execution of this search warrant reflecting the shipment, transfer or distribution of any package containing software products.

e. All documents and records from August 1, 2003 through the date of the execution of this search warrant constituting or referencing communications (whether oral, written or electronic) to, by or between James and Ilona Cochran and any software manufacturers, resellers and/or distributors.

f. All documents, notes, records and tangible things referencing or mentioning CW TECH, James and Ilona Cochran, and/or any of their aliases listed in this affidavit, and any of their software customers and/or software distributors.

g. All documents and records from August 1, 2003 through the date

of the execution of this search warrant for any financial transactions involving CW TECH, James or Ilona Cochran, or any of their aliases listed in this affidavit, or any accounts held by any of these individuals and/or entities at any financial institution.

h. All records, documents, programs, applications, and materials referencing the production, distribution, transfer or procurement of genuine or counterfeit computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) or genuine or counterfeit software licenses (such as client access licenses or end user licenses).

i. All documents, records and tangible things, including bills, letters, invoices, and personal effects, tending to show ownership, occupancy, or control of THE SUBJECT BUSINESS located at 8801 La Mesa Boulevard, La Mesa, California 91941 and/or THE SUBJECT RESIDENCE, located at 1102 La Mesa Boulevard, Spring Valley, California 91977, or any of the above-described items;

j. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form.

k. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the

ability to preserve the data.

ii. If the computer personnel determine it is not practical to perform an on-site search of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iii. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.


iv. If the computer personnel determine that the data does not fall within any of the items to be seized pursuant to this warrant or is not otherwise legally seized, the government will return these items within a reasonable period of time.

1. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

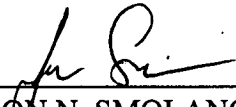
- ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
- iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
- iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;
- v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;
- vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
- vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

28. The government also seeks permission to have non-law enforcement personnel present during the execution of the requested search warrants -- specifically, representatives from Microsoft Corporation, Symantec Corporation and Adobe who have received training and experience from their respective companies in identifying counterfeit software and counterfeit computer and/or software documentation -- for the

purpose of identifying counterfeit software and computer-related documentation, as well as any genuine, but altered software and computer-related documentation, and any production equipment, devices and implements used in the manufacturing and/or altering of such items, *as provided for at Title 18, United States Code, § 3705* 

29. Based on the foregoing facts, I respectfully submit that there is probable cause to believe that JAMES AND ILONA COCHRAN, aka Continuous Wave Technologies, aka CW TECH, have engaged in violations of criminal conspiracy, trademark and copyright laws, namely violations of 18 USC § 2318 (trafficking in counterfeit labels and computer documentation), 18 USC § 2320 (trafficking in counterfeit goods and services), and 17 U.S.C. § 506 (criminal copyright infringement).

30. Based on the foregoing facts, I further respectfully submit that there is probable cause to search the above specified locations and to seize evidence, contraband, and/or instrumentalities of the specified crimes.

  
 JASON N. SMOLANOFF  
 Special Agent  
 Federal Bureau of Investigation

Sworn to before me and subscribed  
 this 22 day of August, 2005.

  
 HON. NITA L. STORMES  
 UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

**Premises To Be Searched -- THE SUBJECT RESIDENCE - 1102 La Mesa**

**Boulevard, Spring Valley, California**



## **ATTACHMENT B**

### **Items To Be Seized**

Items constituting evidence of violations of Title 18, United States Code, Sections 371, 2318 and 2320, including the following:

- a. All computer software, computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) and software licenses (such as client access licenses or end user licenses) bearing any identifying label or mark used by Microsoft, Symantec or Adobe that appears genuine, but is not.
- b. All computer software, computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) and software licenses (such as client access licenses or end user licenses) determined to be, or suspected by appearance and/or price to be, counterfeit, fraudulently obtained, or altered.
- c. All tools, devices, implements, materials, mechanical equipment and tangible things capable of being used in connection with processes to replicate, manufacture, label or otherwise produce documents that appear virtually indistinguishable from genuine computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) and software licenses (such as client access licenses or end user licenses) offered by Microsoft, Symantec or Adobe.
- d. All documents and records from August 1, 2003 through the date of execution of this search warrant reflecting the shipment, transfer or distribution of any package containing software products.

e. All documents and records from August 1, 2003 through the date of the execution of this search warrant constituting or referencing communications (whether oral, written or electronic) to, by or between James and Ilona Cochran and any software manufacturers, resellers and/or distributors.

f. All documents, notes, records and tangible things referencing or mentioning CW TECH, James and Ilona Cochran, and/or any of their aliases listed in this affidavit, and any of their software customers and/or software distributors.

g. All documents and records from August 1, 2003 through the date of the execution of this search warrant for any financial transactions involving CW TECH, James or Ilona Cochran, or any of their aliases listed in this affidavit, or any accounts held by any of these individuals and/or entities at any financial institution.

h. All records, documents, programs, applications, and materials referencing the production, distribution, transfer or procurement of genuine or counterfeit computer documentation (such as certificates of authenticity and manuals designed to be packaged with software) or genuine or counterfeit software licenses (such as client access licenses or end user licenses).

i. All documents, records and tangible things, including bills, letters, invoices, and personal effects, tending to show ownership, occupancy, or control of THE SUBJECT BUSINESS located at 8801 La Mesa Boulevard, La Mesa, California 91941 and/or THE SUBJECT RESIDENCE, located at 1102 La Mesa Boulevard, Spring Valley, California 91977, or any of the above-described items;

j. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials



created, modified or stored in any form.

k. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

ii. If the computer personnel determine it is not practical to perform an on-site search of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iii. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

iv. If the computer personnel determine that the data does not fall within any of the items to be seized pursuant to this warrant or is not otherwise

legally seized, the government will return these items within a reasonable period of time.

I. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

- i. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;
- ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
- iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
- iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;
- v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;
- vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

Non-law enforcement personnel representatives from Microsoft Corporation, Symantec Corporation and Adobe may assist the FBI during execution of the search warrant for the purpose of identifying any counterfeit software and computer-related documentation, as well as any genuine, but altered software and computer-related documentation, and any equipment, devices, materials, implements and other tangible things used in the manufacturing and/or altering of such items, *as provided for at Title 18, United States Code, § 3105.*